National Security Agency/Central Security Service

INFORMATION ASSURANCE DIRECTORATE

CGS Data Protection Capability

Version 1.1.1

Data protection is protecting all data so that it is available when requested and only authorized users may access, modify, destroy, or disclose the data. Data protection is enforced in all data states including in use, at rest, and in transit. Data in use refers to data that is being acted upon. Data at rest refers to data that is being stored. Data in transit refers to data being transferred between systems.

07/30/2012

CGS Data Protection Capability

Version 1.1.1

Table of Contents

1 Revisions

Name	Date	Reason	Version
CGS Team	30 June 2011	Initial release	1.1
CGS Team	30 July 2012	Inclusion of new IAD document template & Synopsis	1.1.1

2 Capability Definition

The Capability definition provides an understanding of the importance of the Capability to the Enterprise. It provides a high-level overview of the Capability based on definitions derived from Committee on National Security Systems (CNSS) Instruction No. 4009.

Data protection is protecting all data so that it is available when requested and only authorized users may access, modify, destroy, or disclose the data. Data protection is enforced in all data states including in use, at rest, and in transit. Data in use refers to data that is being acted upon. Data at rest refers to data that is being stored. Data in transit refers to data being transferred between systems.

3 Capability Gold Standard Guidance

The Capability Gold Standard Guidance evaluates the Enterprise needs and overlays the expected Gold Standard behavior. The guidance goes beyond the concept of “good enough” when describing the Gold Standard recommendations, considers industry best practices, and describes a level of security that not only meets current standards but also exceeds them across the Enterprise.

Enterprise has information that needs to be protected. Protection means that the appropriate controls are in place to prevent unauthorized access, modification, destruction, and disclosure. Data shall remain protected while in use, at rest, and in transit. Regardless of what state the data is in, all security protections shall still apply, such as those provided under the System Protection and Communication Protection Capabilities, among others.

Data in transit includes all data that is transported inside and outside of the Enterprise. When data is transported outside of the Enterprise, it shall be protected in transport such that it can be accessed or modified only by authorized users. The first level of protection shall be provided by the Communication Protection Capability; however, there may be special protections required on the data that go beyond the transport layer protection mechanisms. The Attribute Management Capability shall be leveraged to properly identify protections based on the attributes of the data. Attributes shall include classification and compartment handling, data type, and the recipient of the access control decision. For example, Top Secret (TS) data shall be protected by Type 1 protection mechanisms. Each attribute drives the type of data protection mechanism that is required for the Enterprise.

Data at rest includes data that is stored on storage units, which includes data stored on removable or portable media and backup data. Data at rest shall be protected by physical and logical mechanisms such as encryption. The appropriate level of encryption shall be determined based on applicable policies. In addition, all encryption mechanisms shall be interoperable with peer Enterprise.

When determining how to protect data stored on removable media and portable devices, where the data is going and the environment it shall be stored in shall be considered. Any media that is removable has a higher probability of leaving the environment; therefore, higher levels of protection shall be in place. All removable media shall be encrypted. When a hardware device has the capability to encrypt and can be automated, those mechanisms shall be used as opposed to requiring the user to perform the encryption by use of an application on the data host. Some environments may require exceptions if the stated protection level is not feasible based on the operational environment and mission supported.

Current backups shall be maintained in case there is data loss or accidental or malicious modification. Data backup shall occur regularly to maintain availability requirements and to ensure data that is lost can be recovered. Handling and storage decisions shall be made based on the environment and an analysis of the data attributes such as classification/compartment handling, data type, data relevance, and data functionality to apply appropriate protection mechanisms.

Data in use requires mechanisms to protect data that is acted upon from processes outside of the application. Persistent enforcement of dissemination and use restrictions on data shall be provided. Access control shall be invoked to ensure access is limited to only processes allowed to use the data. The Access Management and System Protection Capabilities work with the Data Protection Capability to ensure that applications can access authorized memory spaces.

The integrity of all data shall be assured to verify that the data has not been modified in an unauthorized manner. Integrity shall be maintained and provide assurance, through the use of cryptographic hash functions and digital signatures, or by the use of cryptographic binding (which uses these technologies), that data has not been altered. Integrity checking occurs for data in storage, before and after each use, and before and after any data transfers. In addition, integrity checks are performed on all data backups.

The Data Protection Capability employs automated mechanisms for data marking and verification and leverages the Metadata Management Capability for tagging data. The Access Management and Attribute Management Capabilities both provide information used to understand where authorization comes from to help determine the level of needed protections and to ensure that information marking controls are applied. For data requiring higher levels of protection, automated handling controls to prevent loss or compromise of data shall be used.

The Data Protection Capability also relies on the proper handling of the data by its users. Users shall be made aware of their responsibilities with respect to data handling to prevent the loss or compromise of data.

4 Environment Pre-Conditions

The environment pre-conditions provide insight into environmental, user, and technological aspects needed for Capability implementation. These pre-conditions are services or other Capabilities that must be in place within the Enterprise for the Capability to function.

1. There are provisions for secure storage of the data and backup media.
2. Users are authenticated and authorizations are verified before gaining access to data.
3. Physical facilities are kept secure and guarded.
4. The Enterprise specifies an audit procedure for backups.
5. The Enterprise provides secure communication protocols to protect the data.
6. The Enterprise provides necessary encryption mechanisms.
7. An authorized data source and policies are in place to determine how to classify and protect data.

5 Capability Post-Conditions

The Capability post-conditions define what the Capability will provide. They define functions that the Capability will perform or constraints that the Capability will operate under when performing its function.

1. The Capability ensures that data at rest, in transit, and in use is protected based on its required protection and security level.
2. The Capability applies classification markings to documents based on policy decisions.
3. The Capability ensures protection mechanisms are interoperable with partner organizations.

6 Organizational Implementation Considerations

Organizational implementation considerations provide insight into what the Organization needs to establish, ensure, and have in place for the specified Capability to be effective. It provides guidance specific to the actions, people, processes, and departments that an Organization will need to execute or establish to implement the guidance described in Section 3 (Capability Gold Standard Guidance).

Each Organization will protect data while in use, at rest, and in transit. When transporting data outside of the Enterprise, Organizations will provide protection, as defined in the Communication Protection Capability, through the infrastructure (e.g., T1) or secure transfer protocols such as Transport Layer Security (TLS) to ensure that data cannot be viewed, modified, or destroyed by unauthorized users.

There may be special protections on the data that go beyond the transport layer protection mechanisms. Inside the payload itself, data recipient and data type will drive the additional protection mechanisms. Whether data in transit is inside or outside of the Enterprise, the Organization will look at classification/compartmental handling needs to determine what additional data protections need to be in place. For example, Top Secret data will require Type 1 protection mechanisms. In addition, operational data will require a higher level of protection than test data. Each of these attributes will drive the type of data protection mechanism the Organization requires. Each Organization will review appropriate policies to determine the appropriate encryption levels (see policy table).

The Organization will prevent loss and corruption of data to ensure it remains recoverable and usable. One way of preventing loss and corruption of data is to encrypt data at rest and use cryptographic bindings. Data integrity-based solutions, such as cryptographic binding, will be used by the Organization to prevent a malicious program or a hacker from modifying data and to provide strong protection against tampering and unauthorized access. Cryptographic binding provides integrity and authenticity to the relationship between a data asset and its associated metadata, thus giving consumers assurance that any malicious or accidental changes in either are detected and that the identity of the entity that created the binding is authenticated, therefore preventing forgery.

Each Organization will encrypt data on all removable media and portable devices. When a portable hardware device (e.g., USB Token) has the capability to encrypt, this capability will be enabled and in use. When available, an Organization will use those

devices as opposed to requiring the user to perform the encryption via an application on the data host. If encryption capabilities do not exist on the device, the Organization will ensure appropriate application-level protections are in place. Organizations will look at the mission needs and their operational environment to enable effective decision-making for application of protections based on environmental risks.

To remove data from media, the Organization will implement data erasure mechanisms, which is a method of overwriting that completely destroys all electronic data residing on a hard drive or other digital media to ensure that no sensitive data remains when an asset is retired or reused. Organizations will use hardware-based erasures and the hardware overwrite process. For an actual system, Organizations will employ protections within the System Protection Capability to ensure proper sanitization techniques are applied. This will be done in accordance with policy because each Organization may require a different number of overwrites (see policy table). For some data protection levels and some organizations, the media will be restricted from being reused and will need to be destroyed.

The Organization will back up data regularly to maintain availability requirements and to ensure that lost data can be recovered to support continuity of operations. The data will be protected to the level of the data, regardless of origination. The Organization will make handling and storage decisions based on the environment in which the data will be stored and based on an analysis of the data attributes such as classification/compartmental handling, data type, and data functionality. Depending on the solution an Organization uses, a higher level of protection will need to be used (e.g., additional encryption requirements).

The Organization will provide persistent enforcement of dissemination and use restrictions on data and access control to ensure access is limited to only processes allowed to use the data. This will be accomplished through the Access Management and System Protection Capabilities. In addition, each Organization will provide IA Awareness Training for its users to ensure they understand proper handling responsibilities and where they are allowed to send data.

The Organization will use a system to analyze data assets and make suggestions on how to classify the asset based on a set of rules and use automated mechanisms for data tagging and verification at every save. To enable data protection, each Organization will leverage the Metadata Management Strategy for tagging data, along with Access and Attribute Management to understand where authorization comes from

to determine the level of needed protections and to ensure that information marking controls are applied.

7 Capability Interrelationships

Capability interrelationships identify other Capabilities within the Community Gold Standard framework that the Capability in this document relies on to operate. Although there are many relationships between the Capabilities, the focus is on the primary relationships in which the Capabilities directly communicate with or influence one another.

7.1 Required Interrelationships

The following Capability interrelationships include the other Capabilities within the Community Gold Standard framework that are necessary for the Capability in this document to operate.

- Understand Data Flows–The Data Protection Capability relies on the Understand Data Flows Capability to provide information used to determine protection requirements and the type of data protection mechanisms that should be used.
- System Protection–The Data Protection Capability relies on the System Protection Capability to provide protection to the systems where data is stored or processed.
- Communication Protection–The Data Protection Capability relies on the Communication Protection Capability to provide protection to the communication links used by data in transit.
- Physical and Environmental Protections–The Data Protection Capability relies on the Physical and Environmental Protections Capability to provide physical protection mechanisms to data.

7.2 Core Interrelationships

The following Capability interrelationships include the Capabilities within the Community Gold Standard framework that relate to every Capability.

- Portfolio Management–The Data Protection Capability relies on the Portfolio Management Capability to determine current and future investment needs and prioritize investments based on those needs.
- IA Policies, Procedures, and Standards–The Data Protection Capability relies on the IA Policies, Procedures, and Standards Capability to provide information about applicable federal laws, Executive Orders, regulations, directives, policies, procedures, and standards.

- IA Awareness–The Data Protection Capability relies on the IA Awareness Capability for an awareness program to inform personnel of their responsibilities related to IA.
- IA Training–The Data Protection Capability relies on the IA Training Capability to provide training programs related to IA activities in accordance with agency policies.
- Organizations and Authorities–The Data Protection Capability relies on the Organizations and Authorities Capability to establish the relevant roles and responsibilities.

7.3 Supporting Interrelationships

The following Capability interrelationships include the other Capabilities within the Community Gold Standard framework that are not necessary for the Capability to operate, although they support the operation of the Capability in this document.

- Hardware Device Inventory–The Data Protection Capability relies on the Hardware Device Inventory Capability to provide information about all of the hardware devices on the network, which is used to determine protection requirements.
- Software Inventory–The Data Protection Capability relies on the Software Inventory Capability to provide information about all of the software assets on the network, which is used to determine protection requirements.
- Risk Analysis–The Data Protection Capability establishes protection mechanisms that are part of an accredited system and documented as such through a certification and accreditation process conducted by the Risk Analysis Capability.
- Risk Mitigation–The Data Protection Capability implements individual countermeasures that may be selected by the Risk Mitigation Capability.

8 Security Controls

This section provides a mapping of the Capability to the appropriate controls. The controls and their enhancements are granularly mapped according to their applicability. In some instances, a control may map to multiple Capabilities.

Control Number/Title	Related Text
NIST SP 800-53 Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*	
AC-3 *ACCESS ENFORCEMENT*	Enhancement/s: (6) The organization encrypts or stores off-line in a secure

	location [Assignment: organization-defined user and/or system information].
AC-4 *INFORMATION FLOW ENFORCEMENT*	Control: The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy. Enhancement/s: (1) The information system enforces information flow control using explicit security attributes on information, source, and destination objects as a basis for flow control decisions. (2) The information system enforces information flow control using protected processing domains (e.g., domain type-enforcement) as a basis for flow control decisions. (3) The information system enforces dynamic information flow control based on policy that allows or disallows information flows based on changing conditions or operational considerations. (4) The information system prevents encrypted data from bypassing content-checking mechanisms. (5) The information system enforces [Assignment: organization-defined limitations on the embedding of data types within other data types]. (6) The information system enforces information flow control on metadata. (7) The information system enforces [Assignment: organization-defined one-way flows] using hardware mechanisms. (8) The information system enforces information flow control using [Assignment: organization-defined security policy filters] as a basis for flow control decisions. (9) The information system enforces the use of human review for [Assignment: organization-defined security policy filters] when the system is not capable of making an information flow control decision. (16) The information system enforces security policies regarding information on interconnected systems.
AC-22 *PUBLICLY ACCESSIBLE*	Control: The organization: a. Designates individuals authorized to post information onto

CONTENT	an organizational information system that is publically accessible. c. Reviews the proposed content of publicly accessible information for nonpublic information prior to posting onto the organizational information system; d. Reviews the content on the publicly accessible organizational information system for nonpublic information [Assignment: organization-defined frequency]; and e. Removes nonpublic information from the publicly accessible organizational information system, if discovered. Enhancement/s: None Specified
CP-9 *INFORMATION SYSTEM BACKUP*	Control: The organization: a. Conducts backups of user-level information contained in the information system [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives]; b. Conducts backups of system-level information contained in the information system [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives]; c. Conducts backups of information system documentation including security-related documentation [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives]; and d. Protects the confidentiality and integrity of backup information at the storage location. Enhancement/s: (5) The organization transfers information system backup information to the alternate storage site [Assignment: organization-defined time period and transfer rate consistent with the recovery time and recovery point objectives]. (6) The organization accomplishes information system backup by maintaining a redundant secondary system, not collocated, that can be activated without loss of information or disruption to the operation.
IA-6 *AUTHENTICATOR FEEDBACK*	Control: The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by

	unauthorized individuals. Enhancement/s: None Specified
MA-2 *CONTROLLED MAINTENANCE*	Control: The organization: d. Sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs; and Enhancement/s: None Applicable to this capability
MP-2 *MEDIA ACCESS*	Enhancement/s: (2) The information system uses cryptographic mechanisms to protect and restrict access to information on portable digital media.
MP-3 *MEDIA MARKING*	Control: The organization: a. Marks, in accordance with organizational policies and procedures, removable information system media and information system output indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and b. Exempts [Assignment: organization-defined list of removable media types] from marking as long as the exempted items remain within [Assignment: organization-defined controlled areas]. Enhancement/s: None Specified
MP-4 *MEDIA STORAGE*	Enhancement/s: (1) The organization employs cryptographic mechanisms to protect information in storage.
MP-5 *MEDIA TRANSPORT*	Enhancement/s : (4) The organization employs cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.
MP-6 *MEDIA SANITIZATION*	Enhancement/s: (2) The organization tests sanitization equipment and procedures to verify correct performance (4) The organization sanitizes information system media containing Controlled Unclassified Information (CUI) or other sensitive information in accordance with applicable organizational and/or federal standards and policies. (5) The organization sanitizes information system media containing classified information in accordance with NSA

	standards and policies. (6) The organization destroys information system media that cannot be sanitized.
SC-20 *SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)*	Control: The information system provides additional data origin and integrity artifacts along with the authoritative data the system returns in response to name/address resolution queries.
SC-21 *SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER)*	Control: The information system performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources when requested by client systems. Enhancement/s: (1) The information system performs data origin authentication and data integrity verification on all resolution responses whether or not local clients explicitly request this service.
SC-28 *PROTECTION OF INFORMATION AT REST*	Control: The information system protects the confidentiality and integrity of information at rest. Enhancement/s: (1) The organization employs cryptographic mechanisms to prevent unauthorized disclosure and modification of information at rest unless otherwise protected by alternative physical measures.
SC-33 *TRANSMISSION PREPARATION INTEGRITY*	Control: The information system protects the integrity of information during the processes of data aggregation, packaging, and transformation in preparation for transmission.
SI-4 *INFORMATION SYSTEMS MONITORING*	Enhancement/s: (8) The organization protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion.
SI-10 *INFORMATION INPUT VALIDATION*	Control: The information system checks the validity of information inputs. Enhancement/s: None Specified.
SI-12 *INFORMATION OUTPUT HANDLING AND RETENTION*	Control: The organization handles and retains both information within and output from the information system in accordance with applicable federal laws, Executive Orders, directives,

	policies, regulations, standards, and operational requirements. Enhancement/s: None Specified

9 Directives, Policies, and Standards

This section identifies existing federal laws, Executive Orders, regulations, directives, policies, and standards applicable to the Capability but does not include those that are agency specific.

Data Protection Directives and Policies

Title, Date, Status	Excerpt / Summary
Intelligence Community (IC)	
ICPM 2007-500-3, Intelligence Information Sharing, 22 December 2007, Unclassified	Summary: Policy: To maximize the dissemination of intelligence information to Intelligence Community (IC) customers relevant to their missions, while balancing the obligation to protect intelligence sources and methods, the IC elements shall: … b. Implement Director of National Intelligence (DNI) approved information technology, personnel/physical security standards, and procedures for providing and protecting intelligence information.
Intelligence Community Information Assurance Architecture, Version 1.1 (final draft), 30 September 2010, Classified	Summary: This document provides Enterprise-level architectural direction and guidance to the implementation of the information assurance (IA) capabilities identified within the IA Concept of Operations (CONOPS), decomposes and describes the IA functions and services that make up these IA capabilities, and describes their evolution from the current As-Is environment to a To-Be objective environment.
Comprehensive National Cybersecurity Initiative (CNCI)	
NSPD-54/HSPD-23 Cybersecurity Presidential Directive (Comprehensive National Cybersecurity Initiative [CNCI]), 8 January 2008, Classified	Summary: National Security Presidential Directive-54/Homeland Security Presidential Directive-23 (NSPD-54/HSPD-23), in which the Comprehensive National Cybersecurity Initiative (CNCI) is described, is classified. Initiative 7 deals with increasing the security of classified networks.
Department of Defense (DoD)	

DoDI 5200.01, DoD Information Security Program and Protection of Sensitive Compartmented Information, 9 October 2008, Unclassified	Summary: This instruction updates policy and responsibilities for collateral, Special Access Program (SAP), Sensitive Compartmented Information (SCI), and controlled unclassified information (CUI) within an overarching DoD Information Security Program.
DoD 5200.1-R, Information Security Program, 14 January 1997, Unclassified	Summary: This document establishes the Department of Defense (DoD) Information Security Program to promote proper and effective classification, protection, and downgrading of official information requiring protection in the interest of national security.
DoD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM), 28 February 2006, Unclassified	Summary: This manual prescribes the requirements, restrictions, and other safeguards to prevent unauthorized disclosure of classified information.
DoDD 8000.01, Management of the DoD Information Enterprise, 10 February 2009, Unclassified	Summary: It is DoD policy that: a. Information shall be considered a strategic asset to the DoD; it shall be appropriately secured, shared, and made available throughout the information lifecycle to any DoD user or mission partner to the maximum extent allowed by law and DoD policy. … d. Information solutions shall provide reliable, timely, accurate information that is protected, secure, and resilient against information warfare, terrorism, criminal activities, natural disasters, and accidents.
DoD Instruction 8520.2, Public Key Infrastructure (PKI) and Public Key (PK) Enabling, 1 April 2004, Unclassified	Summary: This instruction implements policy, assigns responsibilities, and prescribes procedures for developing and implementing a department-wide Public Key Infrastructure (PKI) and enhancing the security of DoD information systems by enabling these systems to use PKI for authentication, digital signatures, and encryption. It aligns DoD PKI and Public Key (PK) enabling activities with DoD Directive 8500.1, as implemented by DoD Instruction 8500.2, and the DoD Common Access Card (CAC) program, as specified by DoD Directive 8190.3.

DoD Memorandum, Encryption of Sensitive Unclassified Data at Rest on Mobile Computing Devices and Removable Storage Media, 3 July 2007, Unclassified	Summary: This memorandum provides for the protection of sensitive unclassified information on mobile computing devices and removable storage media on all DoD components and their supporting commercial contractors that process sensitive DoD information.
DISA Network Infrastructure Secure Technical Implementation Guide (STIG), version 7.1, 25 October 2007, Unclassified	Summary: This guide provides security considerations at the network level needed to achieve an acceptable level of risk for information as it is transmitted through an enclave. It was developed to enhance the confidentiality, integrity, and availability of sensitive DoD automated information systems.
DISA Enclave Security Technical Implementation Guide (STIG), version 4.2, 10 March 2008, Unclassified	Summary: This guide provides Organizations an overview of the applicable policy and additional Secure Technical Infrastructure Guide (STIG) documents required to implement secure information systems and networks while ensuring interoperability.
Committee for National Security Systems (CNSS)	
CNSSP-21, National Information Assurance Policy on Enterprise Architectures for National Security Systems, March 2007, Unclassified	Summary: Federal department and agency Enterprise architectures (EA) shall integrate IA capabilities to mitigate risks associated with national security information. Security controls shall be incorporated at the component, system, service, and application levels of EAs, including plans to manage risk, protect privacy, and provide availability, integrity, authentication, confidentiality, and non-repudiation as part of an integrated IA approach.
Other Federal (OMB, NIST, …)	
DHS Management Directive 11045, Protection of Classified National Security Information:	Summary: This directive prescribes the safeguarding requirements of the classified national security information program within the Department of Homeland Security (DHS) to prevent unauthorized and unnecessary access to classified information.

Accountability, Control, and Storage, 4 October 2004, Unclassified	
Executive Branch (EO, PD, NSD, HSPD, …)	
EO 13526, Classified National Security Information, 29 December 2009, Unclassified	Summary: This document prescribes a uniform system for classifying, safeguarding, and declassifying national security information, including information relating to defense against transnational terrorism.
Legislative	
Public Law 107-347, E.-Government Act, 17 December 2002, Unclassified	Summary: This Public Law was enacted to enhance the management and promotion of electronic government services and processes. It requires the development of EAs within and across the Federal Government, and the provision of information security protections commensurate with the risk and magnitude of the harm resulting from information systems' corruption. It is divided into five titles. The Federal Information Security Management Act of 2002 (FISMA) was enacted as Title III of the E-Government Act. The Act recognized the importance of information security to the economic and national security interests of the United States and requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

Data Protection Standards

Title, Date, Status	**Excerpt / Summary**
Intelligence Community (IC)	
Nothing found	
Comprehensive National Cybersecurity Initiative (CNCI)	

Nothing found	
Department of Defense (DoD)	
Joint DoDIIS/Cryptologic SCI Information Systems Security Standards, Revision 4, 1 January 2006, Unclassified	Summary: This standard provides procedural guidance for the protection, use, management, and dissemination of Sensitive Compartmented Information (SCI). The combination of security safeguards and procedures used for information systems shall achieve U.S. government policy that all classified information must be appropriately safeguarded to ensure the confidentiality, integrity, and availability of that information.
Committee for National Security Systems (CNSS)	
Nothing found	
Other Federal (OMB, NIST, …)	
NIST Special Publication 800-88, Guidelines for Media Sanitization, September 2006, Unclassified	Summary: This special publication assists organizations in implementing a media sanitization program with proper and applicable techniques and controls for sanitization and disposal decisions, considering the security categorization of the associated system's confidentiality.
Executive Branch (EO, PD, NSD, HSPD, …)	
Nothing found	
Legislative	
Nothing found	
Other Standards Bodies (ISO, ANSI, IEEE, …)	
Nothing found	

10 Cost Considerations

This section provides examples of some of the types of costs that the Organization will need to consider when implementing this Capability. The following examples are costs that are common across all of the Community Gold Standards Capabilities:

1. Solution used for implementation (hardware and/or software)

2. Necessary training
3. Licensing (if applicable)
4. Lifecycle maintenance
5. Impact/dependency on existing services
6. Manpower to implement, maintain, and execute
7. Time to implement, maintain, and execute
8. Network bandwidth availability and consumption
9. Scalability of the solution relative to the Enterprise
10. Storage and processing requirements

In addition to the common costs, the following are examples of cost considerations that are specific to this Capability:

1. Cost of backups–Data needs to be backed up and stored in a secure manner.
2. Cost of redundant systems–Additional systems will need to be maintained to provide redundancy.
3. Storage requirements–Storage space must be available for data to reside.

11 Guidance Statements

This section provides Guidance Statements, which have been extracted from Section 3 (Capability Gold Standard Guidance) of this Capability document. The Guidance Statements are intended to provide an Organization with a list of standalone statements that are representative of the narrative guidance provided in Section 3. Below are the Guidance Statements for the [capability name] Capability.

- The Enterprise shall protect all data so that it is available when requested, and only authorized users may access, modify, destroy, or disclose the data. Data protection is enforced in all data states including in use, at rest, and in transit. Data in use refers to data that is being acted upon. Data at rest refers to data that is being stored. Data in transit refers to data being transferred between systems.
- The Enterprise shall protect its data assets while in use, at rest, and in transit.
- When data is transported outside the Enterprise, it shall be protected such that it can be accessed or modified only by authorized users.
- The Enterprise shall leverage an attribute management system to identify protection needs of data based on the associated attributes.
- Attributes for data assets shall include classification, compartment handling, data type, and the recipient of the access control decision.
- Data attributes shall drive the protection mechanisms required for the Enterprise.

- Data at rest shall be protected by physical and logical mechanisms, such as encryption.
- The use of encryption techniques for data protection shall be determined by Enterprise policy.
- Encryption mechanisms shall be interoperable with systems used by peer Organizations.
- The Enterprise shall consider where a data asset is going and the environment in which it is to be stored when determining how to protect data stored on removable media and portable devices.
- All removable media shall be encrypted.
- Encryption mechanisms for the purpose of data protection shall be automated, where possible.
- Exceptions shall be granted, when necessary, if the stated protection level is not feasible based on the operational environment and mission supported.
- Current backups shall be maintained in case there is data loss or accidental or malicious modification.
- Data backup shall occur regularly to maintain availability requirements and to ensure data that is lost can be recovered.
- Handling and storage decisions regarding data backups shall be made based on the environment and an analysis of the data attributes such as classification/compartment handling, data type, data relevance, and data functionality to apply appropriate protection mechanisms.
- The Enterprise shall provide protections for data in use to prevent access from processes outside the authorized application.
- Persistent enforcement of dissemination and use restrictions on data shall be provided.
- Access control shall be invoked to ensure access to data assets is limited to only processes authorized to use them.
- The integrity of all data shall be assured to verify that the data has not been modified in an unauthorized manner.
- Integrity of data assets shall be maintained and provide assurance, through the use of cryptographic hash functions and digital signatures, or by the use of cryptographic binding (which uses these technologies), that data has not been altered.
- Integrity checking occurs for data in storage, before and after each use, and before and after any data transfers.
- Integrity checks shall be performed on all data backups.

- The Enterprise shall employ automated mechanisms for data marking and verification by leveraging a metadata management system for tagging data.
- Automated handling controls shall be used to prevent loss or compromise of data assets that require higher levels of protection.
- Users shall be made aware of their responsibilities with respect to data handling to prevent the loss or compromise of data.